UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

SERGIO BONILLA, on behalf of himself and all others similarly situated,

Plaintiff,

v.

ANCESTRY.COM OPERATIONS INC., a Virginia Corporation; ANCESTRY.COM INC., a Delaware Corporation; ANCESTRY.COM LLC, a Delaware Limited Liability Company; and DOES 1 through 50, inclusive,

Defendants.

CASE NO. 1:20-cv-07390

Hon. Virginia M. Kendall

AGREED STIPULATION AND ORDER GOVERNING THE DISCOVERY OF ELECTRONICALLY STORED INFORMATION

This Agreed Stipulation Governing the Discovery of Electronically Stored Information and Documents ("Protocol") sets forth the specifications that shall govern document production during discovery in the above-captioned action.

SCOPE

1. The parties shall meet and confer to try to resolve any disputes that may arise under this Protocol prior to seeking assistance from the Court.

2. The parties acknowledge that they have an obligation to take reasonable steps to preserve potentially discoverable materials. The parties agree that preservation of potentially relevant materials will be reasonable and proportionate.

3. The parties do not waive any objections to the production, discoverability, or confidentiality of data or any other discovery materials, including without limitation, objections regarding the burden, overbreadth, cost-sharing, or relevance of document requests related to data in a form specified in this Protocol.

4. Nothing herein shall alter the parties' respective responsibility to comply with the applicable Federal Rules of Civil Procedure and any applicable Local Rules regarding the collection or production of data. This Protocol shall neither enlarge, reduce, nor otherwise affect the scope of discovery in this litigation as imposed by the Court's orders nor imply that discovery produced under the terms of this Protocol is properly discoverable, relevant, or admissible in the Action or in any other litigation.

5. In the event the Receiving Party, including any Counsel, Professional Vendor, Expert or other party engaged by the Receiving Party in this Action, experiences a data breach, it shall (to the extent permitted by law) notify the Producing Party as soon as reasonably practicable of the same, and shall reasonably cooperate with the Producing Party to address and remedy the

breach, subject to the Producing Party's reasonable instructions. Nothing herein shall constitute a waiver of legal rights and defenses regarding the protection of information from unauthorized disclosure.

DEFINITIONS

1. "Document" is defined to be synonymous in meaning and equal in scope to the usage of the term in the Federal Rules of Civil Procedure. For avoidance of doubt, the term "document" shall include hard copy documents and electronically stored information.

2. "Hard copy document" means a document that was maintained in paper or other tangible form.

3. "Document family" means a collection of pages or files maintained together constituting a logical single communication of information but consisting of more than a single stand-alone record. Examples include a fax cover, the faxed letter, and an attachment to the letter—the fax cover being the "parent," and the letter and attachment being a "child," or an email and associated attachments, or a presentation with embedded files.

4. "Custodian" shall mean any individual of a producing party identified as likely having possession, custody, or control of potentially relevant documents.

5. "Custodial data source" means any data source used for business purposes in or on which custodian may store potentially relevant documents including, but not limited to, computers, laptops, tablets, and/or mobile devices regularly used for business purposes, email (whether stored locally or centrally), shared network servers, shared or individual network folders, or cloud storage systems.

6. "Non-custodial data source" means any data source that is not kept or maintained by any particular custodian but which may contain relevant documents, including data sources

used by any department, business unit, or division of a producing party, and shared storage systems that may contain relevant documents.

7. "Metadata" means: (i) information embedded in or associated with a file that is not ordinarily viewable or printable from the application that generated, edited, or modified such native file which describes the characteristics, origins, custody, usage, and/or validity of the electronic file; and/or (ii) information generated automatically by the operation of a computer or other information technology system when a native file is created, modified, transmitted, deleted, or otherwise manipulated by a user of such system.

8. "Search term" means a word or a combination of words or phrases designed to capture potentially relevant documents and may include, depending on a data source's capabilities, strings of words or phrases joined by proximity and Boolean connectors or other syntax.

9. "TAR" (technology-assisted review) means a cooperative machine learning process for prioritizing or coding a collection of documents.

10. "Structured data" means data that resides in a fixed field within a record or file, or stored in a structured format, such as databases (such as SAP, JD Edwards, Microsoft Dynamics, Oracle, SQL, Microsoft Access) or data sets, according to specific form and content rules as defined by each field of the database.

PRODUCTION FORMAT

1. To the extent feasible, productions will comply with Exhibit A: Metadata Fields for Electronic Discovery, as well as the below parameters.

2. The parties will produce documents via secure file transfer protocols (e.g., FTP) or similar secure electronic transmission. If a producing party encrypts or "locks" the production,

the producing party shall send, under separate cover or email, an explanation of how to decrypt the files.

3. Electronically stored documents will be produced as searchable PDF files or searchable single-page TIFF files (either extracted text or OCR). Documents produced as searchable PDF files or searchable single-page TIFF files shall correspond to an authentic and complete document (including any concealable information such as formulas or comments) generated by conversion directly from the original native electronic document and shall be accompanied by data load files for loading to Concordance, Summation, or other databases. When it is impracticable for an electronic document to be produced as a PDF or TIFF file, including because any information contained in the document would be omitted, distorted, reorganized, or otherwise made more difficult to read or understand than the document's native format, a party may produce the document in its native format. When it is impracticable for an electronic document (such as a spreadsheet, presentation, or audio file) to be produced as a TIFF file, including because any information contained in the document would be omitted, distorted, reorganized, or otherwise made more difficult to read or understand than the document's native format, a party may produce the document in its native format. Any document or file that is produced in native format must have a corresponding Bates-stamped placeholder TIFF image indicating that a native file has been provided.

4. TIFF images should show any and all text and images which would be visible to the reader using the native software that created the document. For example, TIFF images of email messages should include the BCC line. All other documents or data must be processed to show readily available hidden content, tracked changes or edits, comments, notes, and other similar information for TIFF/JPG images, or alternatively such content must be viewable in the native file.

5. A party may request that specific documents or file types be produced in native format by specifically identifying to the producing party the Bates number of the document sought and the basis for the request for production in native format. A party shall not make unduly burdensome and unreasonable requests for production of documents in native format, and a party shall not unreasonably refuse a request for the production of documents in native format.

6. Bates Numbering. All images must be assigned a unique and sequential Bates Number. The confidentiality designation (if any) corresponding to the confidentiality designations defined in the Protective Order shall appear on each page.

7. Parent-Child Relationships. Responsive non-privileged electronic documents attached to an e-mail or embedded within an electronic document not produced in its native form are to be produced sequentially immediately after the parent document to preserve the parent-child relationship between attachments, enclosures, embedded files, and/or exhibits to any parent document. The child-document should be consecutively produced immediately after the parent-document. If a parent or child is omitted from production as privileged or otherwise, the producing party shall produce in place of the document a single-TIFF placeholder image indicating the withholding of the document and the reason for the withholding.

8. De-Duplication. If a producing party elects to de-duplicate, the producing party shall identify duplicates by the MD5 hash algorithm (or a reasonably equivalent alternative) to create and compare hash values for exact duplicates only. Attachments should not be eliminated as duplicates for purposes of production, unless the parent email and all attachments are also duplicates. An email that includes content in the BCC or other blind copy field should not be treated as a duplicate of an email that does not include content in those fields, even if all remaining content in the email is identical. Custodian-specific de-duplication may be applied to email files

prior to upload to the review platform. Any other de-duplication should be done across the entire collection (i.e., global level) and the "All Custodian" field should list each custodian, separated by a semicolon, who was a source of that document. The "Custodian" field shall represent the custodian of the document uploaded to the review platform.

9. Other De-Duplication Methods. Use of these technologies to reduce the reviewable collection or production, other than as described within this Protocol, requires the producing party to meet and confer with the requesting party.

10. E-mail Thread Suppression. Each party may also de-duplicate emails in such a way as to eliminate earlier or incomplete chains of emails and produce only the most complete iteration of an email chain and any unique attachments associated with the email set, provided that none of the earlier emails in the chain contained attachments and the email chain does not exclude any email conversations that split off from the primary thread. In other words, regardless of the existence of a more complete, later email, all emails that contain attachments must also be produced and all unique email chains should be produced.

11. Redacted Documents. Documents may be redacted to omit privileged information, personal identifying information (PII), information protected or required to be redacted by law, irrelevant information, and information within the scope of Federal Rule of Civil Procedure 5.2.

12. Metadata and Text Files. To the extent feasible, all ESI should be produced with a delimited, database load file that contains the metadata fields listed in Exhibit A hereto, to the extent captured at the time of the collection. To the extent that metadata does not exist or is not reasonably accessible or available because it was overwritten for any documents produced, nothing in this Protocol shall require any party to extract, capture, collect, or produce such data. An .opt

image cross-reference file should also be provided for all TIFF images. The file's extracted text shall also be produced, and OCR shall only be provided when a file requires redaction.

13. Corrupted or Unreadable Files. Each party may exclude certain files that are corrupted or not readable.

14. System Files. Each party may exclude certain files and folders that are reasonably identified as system files and do not contain user-created files.

15. Third-Party-Produced Material. Notwithstanding anything to the contrary herein, any party that produces documents produced to it by a third party, such as in response to a subpoena, may produce such documents in the format in which they were produced by the third party.

16. Color. Documents containing color need not be originally produced in color. If an original document contains color useful to understand the meaning or context of the document, however, the producing party shall honor reasonable requests for either the production of an original document for inspection and copying, or production of a color image of the document. The producing party shall have the option of responding by producing a native-file version of the document. Nothing in this Order shall preclude a producing party from objecting to such requests as unreasonable in number, timing, or scope, provided that a producing party shall not object if the document as originally produced is illegible or difficult to read.

17. Hard Copy Documents. Documents maintained in a party's ordinary course of business as hard copy documents should be scanned in a manner so as to retain the original organization of the hard copy documents. Hard copy documents should be scanned as TIFF images with an .opt image cross-reference file and a delimited database load file (*i.e.*, .dat). The database load file should contain the fields outlined in Exhibit A. Hard copy documents should be

physically unitized. If a producing party reasonably believes that production of hard copy documents is unduly burdensome, the producing party shall seek to meet and confer in good faith with the requesting party regarding content, volume, and related issues before any production of hard copy documents.

18. Original Language. All documents shall be produced in their original language. All extracted text must be produced in a Unicode compliant format in the load file. Nothing in this agreement shall require a producing party to prepare a translation, certified or otherwise, for foreign language documents that are produced in discovery.

CUSTODIANS AND SEARCH METHODOLOGY

19. Structured Data Sources. The producing party may opt to produce relevant and responsive information from databases by querying the database for discoverable information and generating a report in a reasonably usable and exportable electronic format (e.g., in Microsoft Excel™ or .csv format). The parties shall negotiate search methodology, and meet and confer as needed, to be applied to structured data sources. Parties shall agree to search terms to be applied before the producing party collects and produces documents from structured data sources.

20. Determination of Custodians. The parties shall attempt, through a process of cooperative negotiation, to reach agreement on the appropriate number of and identities of custodians. The producing party shall make good faith efforts to provide reasonable information concerning potential custodians as necessary to facilitate these discussions.

21. Custodial and Non-Custodial Data Source Collection. The parties shall negotiate, and meet and confer as needed, concerning the search methodologies to be applied to custodial and non-custodial data sources. Parties shall agree to search terms to be applied before the producing party collects and produces documents from these data sources.

22. Cost-Sharing. The parties also reserve the right to seek and oppose cost-sharing in connection with the collection and production of data that is not reasonably accessible.

ASSERTIONS OF PRIVILEGE

1. Pursuant to Rule 26(b)(5) of the Federal Rules of Civil Procedure, the parties hereby agree that a producing party may redact or withhold a document if it is protected by attorney-client privilege, the work-product doctrine, or any other reasonably applicable privilege from disclosure. Any party that withholds otherwise discoverable information (including by redaction) by claiming that the information is privileged, must produce a log in compliance with Federal Rule of Civil Procedure 26(b)(5). Communications with outside counsel dated after the filing of the first complaint in this Action that are protected by attorney-client or work product privilege do not need to be logged.

2. Should a receiving party be unable to ascertain whether or not a document contained on the log is privileged or have reason to believe a particular entry on the log is responsive and does not reflect privileged information, the parties shall meet and confer as needed to attempt to cooperatively resolve the dispute.

3. Privilege logs shall be produced within thirty days after the relevant production.

4. Nothing in this Protocol shall be interpreted to require disclosure of relevant information or data that is protected by the attorney-client privilege, work-product doctrine, or is prohibited from disclosure under any law, regulation, rule, court order, or any other reasonably applicable privilege or protection. The parties do not waive any objections to the production, discoverability, or confidentiality of data or any other discovery materials, including, without limitation, objections regarding the burden, overbreadth, cost-sharing, or relevance of document requests related to data in a form specified in this Protocol.

5. To the extent that any image file contains information subject to a claim of privilege or any other applicable protection that requires redaction, the portion of the redacted text shall be clearly identified on the face of the TIFF image, either by masking the redacted content with electronic highlighting in black or through the use of redaction boxes. To the extent a document is redacted, OCR text files for such a document shall not contain text for redacted portions. The original unredacted native file shall be preserved pending conclusion of the action. To the extent any native file contains information subject to a claim of privilege or any other applicable protection that requires redactions, the producing party shall either apply the redactions directly on the native file itself or convert that file to TIFF format and produce it with the necessary redactions.

MODIFICATION

1. This Order may be modified by agreement of the parties or by the Court for good cause shown.

IT IS SO STIPULATED, THROUGH COUNSEL OF RECORD.

Exhibit A
Metadata Fields for Electronic Discovery

Field Name	Description	Field Type	Field Value	Non-Email Documents	Emails
ProdBegDoc	Starting Bates (including prefix)	Text	255	X	X
ProdEndDoc	Ending Bates (including prefix)	Text	255	X	X
ProdBegAttach[1]	Starting Bates number of first attachment (including prefix), if applicable	Text	255	X	X
ProdEndAttach	Ending Bates number of last attachment (including prefix), if applicable	Text	255	X	X
Custodian	Custodian or Source, formatted Last, First or ABC Company	Long Text	Unlimited	X	X
All Custodian	Other custodians whose files contained a particular document eliminated through de-duplication	Long Text	Unlimited	X	X
Author	Author of Document, formatted Last, First[2]	Long Text	Unlimited		X
Email_To	Recipient, formatted Last Name, First Name	Multiple Choice	Unlimited		X
Email_From	Author of email formatted, Last Name, First Name	Single Choice	Unlimited		X
Email_CC	Carbon Copy Recipients, formatted Last Name, First Name	Multiple Choice	Unlimited		X
Email_BCC	Blind Carbon Copy Recipients, formatted Last Name, First Name	Multiple Choice	Unlimited		X

[1] Any and all attachments shall be produced sequentially.

[2] Data will be formatted in the manners identified herein to the extent information needed for such formatting is readily available.

DateSent	Date Email was sent, formatted MM/DD/YYYY	Date	MM/DD/YYYY		X
TimeSent	Time Email was sent	Text	10		X
Subject	Subject Line of Email	Long Text	Unlimited		X
NativeLink	Current File Path location to the Native File	Long Text	Unlimited	X	X
TextLink	Current File Path location to the .txt File	Long Text	Unlimited	X	X
File Name	Name of Original File	Text	255	X	X
Hash	MD5 Hash Value	Text	255	X	X
Redaction	Document contains redaction(s)	Text	255	X	X
Confidentiality	Confidential Status of Document	Text	255	X	X

Dated: March 2, 2022

QUINN EMANUEL URQUHART &
SULLIVAN, LLP

By: */s/ Shon Morgan*
Shon Morgan

Shon Morgan (*pro hac vice*)
John W. Baumann (*pro hac vice*)
865 South Figueroa Street, 10th Floor
Los Angeles, CA 90017
(213) 443-3000
shonmorgan@quinnemanuel.com
jackbaumann@quinnemanuel.com

Daniel Lombard
191 N. Wacker Drive, Suite 2700
Chicago, IL 60606
(312) 705-7400
daniellombard@quinnemanuel.com

Cristina Henriquez (*pro hac vice*)
555 Twin Dolphin Drive, 5th Floor
Redwood Shores, CA 94065
(650) 801-5000
cristinahenriquez@quinnemanuel.com

Attorneys for Defendants Ancestry.com Operations Inc., Ancestry.com Inc., and Ancestry.com LLC

Dated: February 28, 2022

LAW OFFICE OF BENJAMIN R. OSBORN

By: */s/ Benjamin R. Osborn*
Benjamin R. Osborn

Shannon M. McNulty
CLIFFORD LAW OFFICES, P.C.
120 N. La Salle, Street, 31st Floor
Chicago, IL 60602
(312) 899-9090
SMM@cliffordlaw.com

Benajmin R. Osborn (*pro hac vice*)
LAW OFFICE OF BENJAMIN R. OSBORN
102 Bergen St.
Brooklyn, NY 11201
(347) 645-0464
ben@benosbornlaw.com

Michael F. Ram (*pro hac vice*)
Marie N. Appel (*pro hac vice*)
MORGAN & MORGAN COMPLEX
LITIGATION GROUP
711 Van Ness Avenue, Suite 500
San Francisco, CA 94102
(425) 358-6913
mram@forthepeople.com
mappel@forthepeople.com

Attorneys for Plaintiff Sergio Bonilla

PURSUANT TO THE AGREED MOTION, IT IS SO ORDERED.

Dated: 3-6-22

Virginia M Kendall

Hon. Virginia M. Kendall
United States District Judge

CERTIFICATE OF SERVICE

I, the undersigned, hereby certify that on March 2, 2022, I caused a true and correct copy of the foregoing to be submitted electronically via e-mail to the Court. All counsel of record were copied on that e-mail.

/s/ Shon Morgan
Shon Morgan